Remarks/Arguments

Claims 1 to 20 are pending in the application. Claims 1 to 20 are rejected.

Claims 1 to 20 remain in the application. Claims 1 to 20 have been amended.

Claims 1, 2, 6, 9-15, 17, 18 have been amended in order to avoid invoking 35 U.S.C. 112, sixth paragraph. In particular, all instances of phrases such as –the step of—have been deleted. Applicant wishes to note for the record that the amendments are neither narrowing, nor are the amendments being made for a reason substantially related to patentability. Applicant respectfully submits that no new matter has been added in the amendments.

Claim 11 has been amended to correct a clerical omission. The word "and" has been added to independent claim 11.

Examiner has requested that the word "password" be inserted after the phrase "from the" in line 12 of claim 1. Claim 1 has been amended to incorporate this change.

Examiner has requested that the article beginning the preambles of dependent claims 2-8, 10 and 12-20 be changed from "A" to "The". The above-mentioned claims have been so modified.

Examiner has requested that the word "identifier" be added after the phrase "the secure password" in line 8 of claim 9. Claim 9 has been amended with this change.

Examiner has requested that the word "the" be replaced with "a" in the second occurrence on line 10 of claim 9. Claim 9 has been amended to recite: "a selected secured file password entry subsystem."

Examiner has requested that the word "a" be replaced with "the" in the preamble of claims 12-20. The preambles of claims 12-20 have been so amended.

Examiner has requested replacement of the word "a" with the word "the" in line 2 of claims 15, 17 and 18. Applicant has not made this change, as it is believed that these instances of "determining **a** plurality of files" and "providing **a** second other password" refer to specific instances of corresponding text provided in claim 11. In these cases Applicant feels that changing "a" to "the" would have undesired effects on the antecedence of these claims. Examiner is respectfully requested to reconsider the proposed amendment.

Examiner has requested that the word "a" on line 3 of claim 20 be deleted and the words "the first" be provided in its place. This amendment has been carried out.

Drawings

Please find replacement pages for all of the drawings. As per request by Examiner, the drawings provided are formalized. Additionally, figure 1 and 2 are now labeled as "prior art". Examiner requested that Fig. 3 and 4 be modified to support a variety of sub-figures 3a-3c and 4a-4d. Applicant is of the opinion that the content of these figures is sufficiently consistent that it does not warrant creating new figures and modifying the specification accordingly. Instead, Applicant has provided a common border around all elements of Fig. 3 and Fig. 4.

Claim Rejections

Claim Rejections - 35 USC § 112

Claims 7 and 8 have been rejected under 35 U.S.C. 112 as being indefinite. Both claims 7 and 8 have been amended to recite, "...the determined system or file" instead of, "the protected file." Therefore claims 7 and 8 now comply with 35 U.S.C. 112. Examiner is respectfully requested to withdraw the rejection.

Claim Rejections - 35 USC § 102

Examiner has rejected claims 11 and 15-19 as being anticipated under 35 U.S.C. 102(e) as being anticipated by US patent #6,182,229 B1 (Nielson).

Claim 11 states:

> *"A method of changing a first password for securing files accessible by password data entry comprising:*
> *determining a plurality of files secured with the first password;*
> *providing a second other password for securing the plurality of files;*
> *for each file secured with the first password, accessing the file with the first password an securing the file with the second other password;*
> *storing the second other password in a password database."*

Referring to the office action provided by Examiner on page 14, beginning on the last line,

> *"providing a second other password for securing the plurality of files (see col. 3 lines 21-24 disclose a master password that being used to encrypt the passwords for remote server entry and possibly the ids, this master password corresponds to the second password that protects security for the urls by encrypting the access password of the url)..."*

The text cited by Examiner (Nielson, col. 3 lines 21-24) reads,

"Fig. 1B depicts the interconnection of client computer system 10 to remote servers 50, 52 and 54. Fig. 1B depicts the Internet 56 interconnecting remote servers 50, 52 and 54."

Applicant notes that the Nielson reference is an excellent reference relating to the field of the instant invention. In particular, the Nielson reference relates to a password database accessible by a "master password." Applicant's invention will improve the operability of the Nielson implementation by rendering same more user-friendly and more seamless in its operation.

That said, Applicant has reviewed the present rejection but is unable to fully appreciate any relevance to the cited reference. In particular, there appears to be no mention or teachings directed toward, "providing a second other password for securing the plurality of files."

Examiner then cites the same text as being particularly relevant to, "securing the file with the second other password." Again, Applicant fails to appreciate the reasoning proposed by Examiner to justify the rejection.

The cited reference of Nielson describes a system that allows a user to keep a password on a first computer. When the user goes to access a secure file or other secure information on a second computer in communication with the first computer, the user need not provide a password that is specific to the desired file or information. Instead, the user provides a "master password." The master password is then used to access a database of passwords that identifies the secure file or other secure information and determines the correct associated password. Nielson does not teach or suggest modifying a password.

Claim 11 clearly recites,

"for each file secured with the first password, accessing the file with the first password and securing the file with the second other password"

At no point does Nielson specify that a secure file be secured using a "second other password," which in the case of the Nielson cited reference is referred to as the "master password." Instead, the Nielson reference clearly specifies that secure content has an associated password and that the master password is used for retrieving the password associated with the secure content from a database of passwords and user ids. Nielson does not teach or suggest securing the secured content with the master password. The master password of Neilson is only used as input to the database of passwords for providing a decrypted password. In the cited reference of Nielson, only the decrypted password is able to access the secure content. Thus, without access to the database of passwords, the master password would not be expected to provide access to the secure content. Nielson does not teach changing the secure file to be accessible with the master password absent accessing the database of passwords.

Further, at no point in Nielson is it taught or suggested to determine "a plurality of files secured with the first password" as recited in independent claim 11. With this in mind, it is apparent that independent claim 11 is neither anticipated nor obvious in light of Nielson.

Claims 15-19 depend from independent claim 11. As claim 11 is neither anticipated nor obvious it is apparent that claims 15-19 cannot be anticipated or obvious. Examiner is respectfully requested to withdraw the rejection.

Claim Rejections - 35 USC § 103

Applicant would like to point out that in the field of computer security, any security enhancement or enhanced convenience – no matter how small – is often of extreme value, and as such, even very small distinctions are often highly inventive.

Claim 1 clearly recites,

"A method of providing improved security for systems or files accessible by password data entry comprising:
determining a secure password;
providing a system or file;
providing the secure password to a password database independent of the system and the file for storage therein in association with a security level;
providing the secure password to a password sub-system for securing the determined system or file;
determining a user authorisation method having an associated security level sufficient for accessing the secure password, the user authorization method determined in dependence upon the security level and some user authorization methods having different associated security levels than others;
authorising an individual according to the secure authorisation method;
when the individual is authorised, retrieving the secure password from the password database and automatically providing the secure password to the system or file password subsystem for accessing the system or file wherein the system or file is accessible by manually entering the secure password to the password sub-system."

Each cited reference cited relies on password protection as an exclusive teaching. Though other methods of protection are disclosed, they are recited as interchangeable with the password. An understanding of the cited references shows that none of the references teaches the bolded step in claim 1. Applicant is of the opinion that the cited references teach away from implementation of such a step as there is no benefit in determining a user authorization method when there is only one available. In particular, each relies on a predetermined known and assumed authentication method without a step of determining a user authorisation method. Thus, in the teaching of the cited references a specific object becomes accessible once a specific predetermined user authentication process has been carried out.

Clearly, as recited in the present application, it is advantageous to determine a user authorization method in order to store each password within a password database for retrieval in accordance with the determined user authorization method. This renders the system supportive of different authentication methods having different levels of security associated therewith. Such an increased level of security is highly advantageous, though typically inconvenient. Thus, the inventive method as claimed provides for increased inconvenience when security is paramount and increased convenience when security is less important.

Examiner as rejected claim 1 as being obvious under 35 U.S.C. 103(a) in light of the combination of US patent #5,944,824 (He) and US patent #6,618,806 (Brown). The cited reference of He teaches a network that supports "single sign on" allowing a user to securely log into one device of a suitably configured network and have access to a plurality of associated network devices. The "single sign on" clearly supports a single level of security. Specifically, there is no suggestion in He that additional signing on processes are necessary for accessing files or network devices that are designated as highly secure. The invention as recited in amended claim 1 teaches a very different system. Specifically, amended claim 1 now recites:

> *"determining a user authorisation method having an associated security level sufficient for accessing the secure password, the user authorization method determined in dependence upon the security level and some user authorization methods having different associated security levels than others;*
> *authorising an individual according to the secure authorisation method"*

This is fundamentally different from the teachings of He. Specifically, He does not teach "determining a user authorization method having an associated security level sufficient for accessing the secure password." Therefore, it is apparent that a person of skill in the art would not be lead to the invention as described in claim 1 after having reviewed and understood He. As such He does not render the invention as recited in claim 1 obvious.

The cited reference of Brown describes a method of authenticating a user supporting network access. Brown teaches that the individual objects have a specific "rule" associated with their access and that when a rule is not specified another rule is provided based upon a hierarchy of rules (reference Brown column 9, lines 3 to 18.) As described by Brown, each rule has an associated user authentication process (reference Brown column 8, lines 27-50.) While superficially this may seem consistent with claim 1 upon further examination it is apparent that it is not. Specifically, Brown teaches the assumption that anther rule of authentication will be adequate when no rule is otherwise specified. At no point does Brown suggest "determining a user authorisation method having an associated security level sufficient for accessing the secure password, the user authorization method determined in dependence upon the security level and some user authorization methods having different associated security levels than others" as recited in amended claim 1. Thus, in the system of Brown while the rules for authentication are optionally as simple or complex as desired it is not apparent how the rules are to be modified should a change to the rules be desired. Specifically, in the system of Brown if it is determined at some future time that the fingerprint authorization is no longer considered to be adequate to maintain security it is not clear how the rule system of Brown would be modified absent a need to change the rules of Brown. The changing of authentication rules is likely to be a cumbersome task because each object, workstation and system is potentially associated with its own rule (reference Brown column 9 lines 9 to 17.) In contrast, the method of amended claim 1 supports better flexibility because the "user authorisation method" that is determined is associated with an "associated security level sufficient for accessing the secure password" however the user authorisation method is being determined at the time when authentication is desired. As such it is a simple matter for a security administrator to decide that an eight-digit password is no longer an acceptable format for a mid-level user authorisation but that a fingerprint image is, and to implement that change, provided of course that the necessary equipment is deployed in a timely fashion.

In this way, the method of amended claim 1 supports a separation of management for each of user authorisation methods and assessment of security needs for specific objects.

Specifically, an authentication expert decides which user authorisation methods correspond to a given security level and an intelligence expert decides how secure an object should be. This is not obvious based upon the cited reference of Brown.

Examiner has suggested that, in Brown, Fig. 3 and its associated text describe, "determining a user authorisation method having an associated security level sufficient for accessing the secure password." In order to clearly express the differences between the invention as described in claim 1 from the relevant reference, claim 1 has been amended. Thus, claim 1 now recites,

> *"determining a user authorisation method having an associated security level sufficient for accessing the secure password, the user authorization method determined in dependence upon the security level and some user authorization methods having different associated security levels than others"*

authorising an individual according to the secure authorisation method This clearly indicates that a plurality of security levels exist. In the cited reference of Brown as shown in Fig. 3 and the text of column 4, line 58 to column 5, line 30 an authentication method is described in which a same level of security is provided using two different authentication methods. Specifically, in figure 3 of Brown blocks 311 and 319 both correspond to a completed log-in process. Brown does not suggest that these two login processes are otherwise dissimilar.

It is uncertain how a person of skill in the art would combine He and Brown to produce a method consistent with the method recited in claim 1. Specifically, neither He nor Brown teach or suggest a method comprising:

> *"determining a user authorisation method having an associated security level sufficient for accessing the secure password, the user authorization method determined in dependence upon the security level and some user authorization methods having different associated security levels than others"*

As neither He nor Brown teach or suggest this step it is apparent that one of ordinary skill in the art would not lead to combine He and Brown to provide a method that supports such

a step. Thus, it is uncertain what the motivation to combine He and Brown would be. As such, the invention as described with reference to claim 1 is not obvious in light of He and Brown in combination.

Claims 2-4 and 6-10 depend from claim 1. As claim 1 is not obvious in light of He in combination with Brown it is clear that claims 2-4 and 6-10 cannot be obvious in light of He in combination with Brown.

Claim 5 has been rejected as being obvious in light of He in combination with Brown and US patent #6,061,799 (Eldridge.) The cited reference of Eldridge describes a system for storing passwords and updating passwords. Additionally, the cited reference of Eldridge is used for transferring data corresponding to passwords via public keys. Eldridge does not teach or suggest a method comprising:

> *"determining a user authorisation method having an associated security level sufficient for accessing the secure password, the user authorization method determined in dependence upon the security level and some user authorization methods having different associated security levels than others"*

as recited in claim 1. Therefore, it is apparent that Eldridge does not render amended claim 1 obvious. Similarly, as explained hereinabove, the cited reference of He in combination with Brown does not render this same step of amended claim 1 obvious. With this in mind it is not apparent how a person of ordinary skill in the art would combine Eldridge with He and Brown to provide a method consistent amended claim 1. Further, it is not apparent why a person of skill in the art would make the effort to combine them as none of these cited references suggest the advantages of the invention. Claim 5 depends from claim 1 and claim 1 is clearly not obvious in light of the combination of He, Brown and Eldridge. With this in mind, it is apparent that claim 5 is not obvious in light of Eldridge in combination with He and Brown.

Claims 12, 13 and 20 have been rejected under U.S.C. 103 (a) as being obvious in light of Nielson in further view of US patent 6,145,086 (Bellemoor).

As described hereinabove, independent claim 11 is neither anticipated nor obvious in light of Neilson. Claims 12, 13 and 20 all depend from claim 11 and therefore, claims 12, 13 and 20 cannot be obvious in light of Nielson. The cited reference of Bellemoor teaches a system that determines if a password is acceptable in a system that determines access privileges based upon passwords. Unlike Neilson, Bellemoor does describe the notion of maintaining a list of previously used passwords associated with a user. However, Bellemoor does not teach or suggest, "*determining a plurality of files secured with the first password*" as recited in claim 11. The cited reference of Nielson describes a system where a secondary password is associated with an object and a userid after a master password is provided however, Nielson does not teach or suggest, "*determining a plurality of files secured with the first password*" as recited in claim 11. As neither Nielson nor Bellmoor teach or suggest this it is apparent that independent claim 11 is not obvious in light of the cited reference of Nielson in combination with Bellemoor.

As claims 12, 13 and 20 depend from independent claim 11 it is apparent that since independent claim 11 is not obvious in light of the combination of Nielson and Bellemoor dependent claims 12, 13 and 20 cannot be obvious in light of the combination of Nielson and Bellemoor.

Claim 14 has been rejected under U.S.C. 103(a) as being obvious in light of Nielson in combination with Bellemoor and Brown. As described hereinabove independent claim 11 is not obvious in light of the combination of Nielson and Bellemoor. The cited reference of Brown describes a method of authenticating user supporting network access. The cited reference of Brown relies upon a system of rules that supports varying qualities of access to the network as generally described in the abstract of Brown. Referring to Fig. 3 of Brown when a userid is provided the system determines if the userid has a corresponding BIR (biometric identifier record.) If no BIR exists then the user is prompted to provide a password (ref Brown, Fig. 3 309, 311.) If one does exist then the user is prompted to provide a biometric sample (ref Brown, Fig. 3, 307, 313.) In the system of Brown the biometric authentication is clearly used as a convenient and secure option in lieu of a conventional password authentication process. Independent claim 11 recites:

"A method of changing a first password for securing files accessible by password data entry comprising:
determining a plurality of files secured with the first password;
providing a second other password for securing the plurality of files;
for each file secured with the first password, accessing the file with the first password and securing the file with the second other password;
storing the second other password in a password database."

Brown does not teach or suggest "accessing the file with the first password and securing the file with the second other password." Instead, as shown in Fig. 3 of Brown, Brown teaches receiving user identification data and providing access in response to one of providing a valid password and providing appropriate biometric data, which Examiner justifiably considers analogous to providing a second other password. Effectively Brown teaches giving users the opportunity to provide a biometric sample when a suitable biometric scanner is available – a fingerprint and a password are interchangeable. There is no mention of security level associated with the two forms of authorization nor is there a decision between the methods based on the unmentioned security level. Further, Brown does not teach, "determining a plurality of files secured with the first password" as recited in independent claim 11. Thus, it is apparent that independent claim 11 is not obvious in light of Brown.

The cited reference of Nielson teaches a system that supports using a "master password" to provide access to a set of stored passwords associated with specific files, applications or other objects. The cited reference of Bellemoor describes a system that determines if a password is "acceptable" based on a set of predetermined criteria. None of these three cited references suggest any synergy with any of the other cited references. In other words, it is not apparent why a person of ordinary skill in the art would be lead to believe that they should be combined. Thus, it is uncertain what the motivation to combine Brown with Nielson and Bellemoor is. Further, none of Nielson, Bellemoor or Brown teach "determining a plurality of files secured with the first password" and therefore it is apparent that independent claim 11 is not obvious in light of the combination of Nielsen,

Bellemoor and Brown. Claim 14 depends from claim 11 and therefore, claim 14 cannot be obvious in light of the combination of Nielsen, Bellemoor and Brown.

Applicant kindly requests favorable reconsideration of the amended application.

A Petition for Extension of Time is filed concurrently with this response.

Please charge any additional fees required or credit any overpayment to Deposit Account No: 50-1142.

Respectfully,

Gordon Freedman, Reg. No. 41,553

Freedman & Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario K2G 5X3 Canada

Tel: (613) 274-7272
Fax: (613) 274-7414
Email: gordon@freedmanandassociates.ca

VL/sah

Amendments to the Drawings:

The attached sheets of formal drawings replace the original sheets.

Attachment: Figures 1 to 7.